REMARKS

Applicant's remarks, below, are preceded by quotations of the related comments of the examiner (in small, bold-face type) from the examiner's action in the parent case.

> **2. Claims 1-26 are rejected under 35 U.S.C. s. 103 as being unpatentable over Adams, Jr. et al (782), Aziz et al (646), Aziz (842) or Gelb in view of Aziz (362).**
>
> **Each of Adams, Jr. et all (782)(See Figs. 4a-8 and Cols. 9-11) or Aziz et al(646)(See Figs 3-12), Aziz(842)(See Figs. 2-11) or Gelb(See Fig. 1) disclose the network tunneling system including encryption substantially as claimed. It is also noted that each of the above protect downstream internal computer assets through encryption. The differences between the above and the claimed invention is the use of the term "virtual tunnel". While this is believed to be inherent in the primary items of evidence cited as any network connection is virtual, Aziz (See Figs. 1-12) show the changing nature of network tunnels. It would have been obvious to the person having ordinary skill in this art to provide a similar arrangement for Adams, Jr. et al (782), Aziz et al (646), Aziz(842) or Gelb because it is conventional and standard practice to redefine an existing structure as its functional equivalent and these components are no more than the conventional equivalents of what is disclosed in the primary item of evidence. The deficiencies of the art with respect to some of the dependent claims deal with the conventional cryptographic protocols.**

Independent Claim 1

Independent claim 1 has been amended to make clear that the encrypted packet is received from an external network at a first computer and then a determination is made "whether to decrypt the encrypted network packet at the first computer or to pass the encrypted network packet to a computer on a network that is internal with respect to the first computer for decryption." One advantage of this technique is the distribution of decryption processing among different computers on networks internal to the first computer.

None of the cited references shows or suggests passing encrypted packets to a computer on an internal network after

B

determining whether to decrypt the packet at the first computer. Adams, (see Figs. 2 and 8), Gelb (see Fig. 1), and Aziz (842) (see Fig. 3, 5, and 12) show configurations where a single decrypting computer handles all decryption for a network or subnetwork. For example, Aziz 646's TB7 (tunnel bridge 7) in Fig. 12 performs all decryption for packets destined for a computer within subnetwork N12. TB7 does not determine whether it or a computer within subnetwork N12 should decrypt the packet. Either TB7 decrypts the packet or no decryption occurs. Similarly, in Adams Fig. 6, CNEDDs (computer network encryption/decryption devices) 10D and 10E perform decryption for subnetworks 46 and 52, respectively. No nesting of CNEDDs within a subnetwork is shown, let alone a method of determining which CNEDD should perform the encryption. Aziz (842) goes so far as to advocate concentrating decryption functions in a single firewall computer to "minimize[s] the impact of providing key-management facilities in every node." (col. 1, lines 42-45). Neither does Aziz (362) describe or suggest determining whether to decrypt an encrypted network packet or pass the encrypted packet to a computer that is internal with respect to the determining computer.

Independent claim 14

Independent claim 14 recites receiving an encrypted network packet and examining a packet field "to determine which of a plurality of encryption algorithms was used to encrypt the network packet and to determine a destination computer for each

encrypted network packet." One advantage of this technique is that a packet can be routed to a decrypting destination computer without requiring that the decrypting destination computer's network address appear in the packet header. None of the cited references examine a field that represents a method of encryption to determine a destination computer, let alone, postponing decryption until the packet reaches the determined destination computer.

Independent claims 22 and 25

Independent claims 22 and 25 both recite "determining which virtual tunnel each network packet was sent over." Claim 22 further recites "routing each network packet to a destination computer in accordance with the virtual tunnel," while claim 25 further recites "determining whether a source computer that sent each network packet is authorized to send network packets over the determined virtual tunnel."

The examiner incorrectly suggests that the cited references inherently use "virtual tunnels." While Aziz (646), Gelb, and Adams tunnel packets, the tunneling described in these references consists of encapsulating and encrypting packets between a transmitting firewall computer and a single receiving firewall computer. Tunneling packets in this manner can burden the receiving firewall computer with the decryption and decapsulation tasks needed to route packets to their destination. A virtual tunnel that can route a packet past a firewall for

decryption or authentication by a different computer distributes security tasks while keeping the address of the decrypting firewall secret during transmission over the network (i.e., only the address of the first receiving computer need appear in the header or the rest of the packet for that matter). None of the cited references achieve this advantage or inherently contain or suggest the claimed technique.

Independent Claim 24

Independent claim 24 recites "storing a virtual tunnel identifier in the packet that is used to determine routing of the packet." By using the virtual tunnel identifier to determine routing, the network addresses of the encrypting and decrypting computers need not appear in the packet header during transmission over a public network. None of the cited references describe or suggest determining packet routing by examining a virtual tunnel identifier. Instead, the references store the network addresses of the encrypting/encapsulating and decrypting/decapsulating computers in the packet header during packet transmission.

For the reasons discussed above, the cited references failed to anticipate or make obvious the applicant's independent claims. All other dependent claims incorporate features of the independent claims discussed above and therefore are patentable for at least the same reasons.

Applicant asks that all claims be allowed.

Please apply any credits or excess charges to our deposit account number 06-1050.

Respectfully submitted,

Date: 2/9/98

David L. Feigenbaum
Reg. No. 30,378

Fish & Richardson
225 Franklin Street
Boston, MA 02110-2804

Telephone: 617/542-5070
Facsimile: 617/542-8906
280885.B11